Windows PowerShell Get-Help on Cmdlet 'New-AzADAppCredential'

PS:\>Get-HELP New-AzADAppCredential -Full

NAME

New-AzADAppCredential

SYNOPSIS

Creates key credentials or password credentials for an application.

SYNTAX

New-AzADAppCredential -ObjectId <String> [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] [-DefaultProfile <PSObject>] [-Break]

[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials]

[-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential -ObjectId <String> [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] -CertValue <String> [-DefaultProfile

<PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]

[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential -ObjectId <String> [-CustomKeyIdentifier <String>] -KeyCredentials <MicrosoftGraphKeyCredential[]> [-DefaultProfile <PSObject>] [-Break]
[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials]
[-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential -ObjectId <String> [-CustomKeyIdentifier <String>] -PasswordCredentials <MicrosoftGraphPasswordCredential[]> [-DefaultProfile <PSObject>]
[-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] -ApplicationObject <IMicrosoftGraphApplication> [-DefaultProfile
<PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] -CertValue <String> -ApplicationObject
<IMicrosoftGraphApplication> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>]
[-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] -DisplayName <String> [-DefaultProfile <PSObject>] [-Break]
[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials]
[-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] -CertValue <String> -DisplayName <String> [-DefaultProfile
<PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy

<Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] -CertValue <String> -ApplicationId <Guid> [-DefaultProfile
<PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-StartDate <DateTime>] [-EndDate <DateTime>] [-CustomKeyIdentifier <String>] -ApplicationId <Guid> [-DefaultProfile <PSObject>] [-Break]
[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials]
[-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-CustomKeyIdentifier <String>] -PasswordCredentials <MicrosoftGraphPasswordCredential[]> -ApplicationObject <IMicrosoftGraphApplication>
[-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential
<PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-CustomKeyIdentifier <String>] -PasswordCredentials <MicrosoftGraphPasswordCredential[]> -DisplayName <String> [-DefaultProfile <PSObject>]
[-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-CustomKeyIdentifier <String>] -PasswordCredentials <MicrosoftGraphPasswordCredential[]> -ApplicationId <Guid> [-DefaultProfile <PSObject>]
[-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-CustomKeyIdentifier <String>] -KeyCredentials <MicrosoftGraphKeyCredential[]> -ApplicationObject <IMicrosoftGraphApplication> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-CustomKeyIdentifier <String>] -KeyCredentials <MicrosoftGraphKeyCredential[]> -DisplayName <String> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzADAppCredential [-CustomKeyIdentifier <String>] -KeyCredentials <MicrosoftGraphKeyCredential[]> -ApplicationId <Guid> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Creates key credentials or password credentials for an application.

PARAMETERS

-ObjectId <String>

The object Id of application.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-StartDate <DateTime>

The effective start date of the credential usage.

The default start date value is today.

For an 'asymmetric' type credential, this must be set to on or after the date that the X509 certificate is valid from.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-EndDate <DateTime>

The effective end date of the credential usage.

The default end date value is one year from today.

For an 'asymmetric' type credential, this must be set to on or before the date that the X509 certificate is valid.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-CustomKeyIdentifier <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-PasswordCredentials <MicrosoftGraphPasswordCredential[]>

Password credentials associated with the application.

To construct, see NOTES section for PASSWORDCREDENTIALS properties and create a hash table.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-KeyCredentials <MicrosoftGraphKeyCredential[]>

key credentials associated with the application.

To construct, see NOTES section for KEYCREDENTIALS properties and create a hash table.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-CertValue <String>

The value of the 'asymmetric' credential type.

It represents the base 64 encoded certificate.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ApplicationId <Guid>

The application Id.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DisplayName <String>

The display name of application.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ApplicationObject <IMicrosoftGraphApplication>

The application object, could be used as pipeline input.

To construct, see NOTES section for APPLICATIONOBJECT properties and create a hash table.

Required? true

Position? named

Default value

Accept pipeline input? true (ByValue)

Accept wildcard characters? false

-DefaultProfile <PSObject>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

Microsoft.Azure.PowerShell.Cmdlets.Resources.MSGraph.Models.ApiV10.IMicrosoftGraphApplication

OUTPUTS

Microsoft.Azure.PowerShell.Cmdlets.Resources.MSGraph.Models.ApiV10.IMicrosoftGraphKeyCredential

Microsoft.Azure.PowerShell.Cmdlets.Resources.MSGraph.Models.ApiV10.IMicrosoftGraphPasswordCredential

NOTES

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For information on hash tables, run Get-Help

about_Hash_Tables.

APPLICATIONOBJECT <IMicrosoftGraphApplication>: The application object, could be used as pipeline input.

[(Any) <Object>]: This indicates any property can be added to this object.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[AddIn <IMicrosoftGraphAddIn[]>]: Defines custom behavior that a consuming service can use to call an app in specific contexts. For example, applications that

can render file streams may set the addIns property for its 'FileHandler' functionality. This will let services like Office 365 call the application in the

context of a document the user is working on.

[Id <String>]:

[Property <IMicrosoftGraphKeyValue[]>]:

[Key <String>]: Key.

[Value <String>]: Value.

[Type <String>]:

[Api <IMicrosoftGraphApiApplication>]: apiApplication

[(Any) <Object>]: This indicates any property can be added to this object.

[AcceptMappedClaim <Boolean?>]: When true, allows an application to use claims mapping without specifying a custom signing key.

[KnownClientApplication <String[]>]: Used for bundling consent if you have a solution that contains two parts: a client app and a custom web API app. If you

set the appID of the client app to this value, the user only consents once to the client app. Azure AD knows that consenting to the client means implicitly

consenting to the web API and automatically provisions service principals for both APIs at the same time. Both the client and the web API app must be registered

in the same tenant.

[Oauth2PermissionScope <IMicrosoftGraphPermissionScope[]>]: The definition of the delegated permissions exposed by the web API represented by this application

registration. These delegated permissions may be requested by a client application, and may be granted by users or administrators during consent. Delegated

permissions are sometimes referred to as OAuth 2.0 scopes.

[AdminConsentDescription <String>]: A description of the delegated permissions, intended to be read by an administrator granting the permission on behalf of

all users. This text appears in tenant-wide admin consent experiences.

[AdminConsentDisplayName <String>]: The permission's title, intended to be read by an administrator granting the permission on behalf of all users.

[Id <String>]: Unique delegated permission identifier inside the collection of delegated permissions defined for a resource application.

[IsEnabled <Boolean?>]: When creating or updating a permission, this property must be set to true (which is the default). To delete a permission, this

property must first be set to false. At that point, in a subsequent call, the permission may be removed.

[Origin <String>]:

[Type <String>]: Specifies whether this delegated permission should be considered safe for non-admin users to consent to on behalf of themselves, or whether

an administrator should be required for consent to the permissions. This will be the default behavior, but each customer can choose to customize the behavior in

their organization (by allowing, restricting or limiting user consent to this delegated permission.)

[UserConsentDescription <String>]: A description of the delegated permissions, intended to be read by a user granting the permission on their own behalf.

This text appears in consent experiences where the user is consenting only on behalf of themselves.

[UserConsentDisplayName <String>]: A title for the permission, intended to be read by a user granting the permission on their own behalf. This text appears

in consent experiences where the user is consenting only on behalf of themselves.

[Value <String>]: Specifies the value to include in the scp (scope) claim in access tokens. Must not exceed 120 characters in length. Allowed characters are

: ! # $ % & ' ( ) * + , - . / : ; = ? @ [ ] ^ + _ { } ~, as well as characters in the ranges 0-9, A-Z and a-z. Any other character, including the space

character, are not allowed. May not begin with ..

[PreAuthorizedApplication <IMicrosoftGraphPreAuthorizedApplication[]>]: Lists the client applications that are pre-authorized with the specified delegated

permissions to access this application's APIs. Users are not required to consent to any pre-authorized application (for the permissions specified). However, any

additional permissions not listed in preAuthorizedApplications (requested through incremental consent for example) will require user consent.

[AppId <String>]: The unique identifier for the application.

[DelegatedPermissionId <String[]>]: The unique identifier for the oauth2PermissionScopes the application requires.

[RequestedAccessTokenVersion <Int32?>]: Specifies the access token version expected by this resource. This changes the version and format of the JWT produced

independent of the endpoint or client used to request the access token. The endpoint used, v1.0 or v2.0, is chosen by the client and only impacts the version of

id_tokens. Resources need to explicitly configure requestedAccessTokenVersion to indicate the supported access token format. Possible values for

requestedAccessTokenVersion are 1, 2, or null. If the value is null, this defaults to 1, which corresponds to the v1.0

endpoint. If signInAudience on the

application is configured as AzureADandPersonalMicrosoftAccount, the value for this property must be 2

[AppRole <IMicrosoftGraphAppRole[]>]: The collection of roles assigned to the application. With app role assignments, these roles can be assigned to users,

groups, or service principals associated with other applications. Not nullable.

[AllowedMemberType <String[]>]: Specifies whether this app role can be assigned to users and groups (by setting to ['User']), to other application's (by

setting to ['Application'], or both (by setting to ['User', 'Application']). App roles supporting assignment to other applications' service principals are also

known as application permissions. The 'Application' value is only supported for app roles defined on application entities.

[Description <String>]: The description for the app role. This is displayed when the app role is being assigned and, if the app role functions as an

application permission, during consent experiences.

[DisplayName <String>]: Display name for the permission that appears in the app role assignment and consent experiences.

[Id <String>]: Unique role identifier inside the appRoles collection. When creating a new app role, a new Guid identifier must be provided.

[IsEnabled <Boolean?>]: When creating or updating an app role, this must be set to true (which is the default). To delete a role, this must first be set to

false. At that point, in a subsequent call, this role may be removed.

[Value <String>]: Specifies the value to include in the roles claim in ID tokens and access tokens authenticating an assigned user or service principal. Must

not exceed 120 characters in length. Allowed characters are : ! # $ % & ' ( ) * + , - . / : ; = ? @ [ ] ^ + _ { } ~, as well as characters in the ranges 0-9,

A-Z and a-z. Any other character, including the space character, are not allowed. May not begin with ..

[ApplicationTemplateId <String>]: Unique identifier of the applicationTemplate.

[CreatedOnBehalfOfDeletedDateTime <DateTime?>]:

[CreatedOnBehalfOfDisplayName <String>]: The name displayed in directory

[Description <String>]: An optional description of the application. Returned by default. Supports $filter (eq, ne, NOT, ge, le, startsWith) and $search.

[DisabledByMicrosoftStatus <String>]: Specifies whether Microsoft has disabled the registered application. Possible values are: null (default value),

NotDisabled, and DisabledDueToViolationOfServicesAgreement (reasons may include suspicious, abusive, or malicious activity, or a violation of the Microsoft

Services Agreement). Supports $filter (eq, ne, NOT).

[FederatedIdentityCredentials <IMicrosoftGraphFederatedIdentityCredential[]>]: Federated identities for applications. Supports $expand and $filter (eq when

counting empty collections).

[Audience <String[]>]: Lists the audiences that can appear in the external token. This field is mandatory, and defaults to 'api://AzureADTokenExchange'. It

says what Microsoft identity platform should accept in the aud claim in the incoming token. This value represents Azure AD in your external identity provider and

has no fixed value across identity providers - you may need to create a new application registration in your identity provider to serve as the audience of this

token. Required.

[Description <String>]: The un-validated, user-provided description of the federated identity credential. Optional.

[Issuer <String>]: The URL of the external identity provider and must match the issuer claim of the external token being exchanged. The combination of the

values of issuer and subject must be unique on the app. Required.

[Name <String>]: is the unique identifier for the federated identity credential, which has a character limit of 120 characters and must be URL friendly. It is

immutable once created. Required. Not nullable. Supports $filter (eq).

[Subject <String>]: Required. The identifier of the external software workload within the external identity provider. Like the audience value, it has no fixed

format, as each identity provider uses their own - sometimes a GUID, sometimes a colon delimited identifier, sometimes arbitrary strings. The value here must

match the sub claim within the token presented to Azure AD. The combination of issuer and subject must be unique on the app. Supports $filter (eq).

[GroupMembershipClaim <String>]: Configures the groups claim issued in a user or OAuth 2.0 access token that the application expects. To set this attribute, use

one of the following string values: None, SecurityGroup (for security groups and Azure AD roles), All (this gets all security groups, distribution groups, and

Azure AD directory roles that the signed-in user is a member of).

[HomeRealmDiscoveryPolicy <IMicrosoftGraphHomeRealmDiscoveryPolicy[]>]:

[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[AssignedPlan <IMicrosoftGraphAssignedPlan[]>]: The collection of service plans associated with the tenant. Not nullable.

[AssignedDateTime <DateTime?>]: The date and time at which the plan was assigned. The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z.

[CapabilityStatus <String>]: Condition of the capability assignment. The possible values are Enabled, Warning, Suspended, Deleted, LockedOut. See a

detailed description of each value.

[Service <String>]: The name of the service; for example, exchange.

[ServicePlanId <String>]: A GUID that identifies the service plan. For a complete list of GUIDs and their equivalent friendly service names, see Product

names and service plan identifiers for licensing.

[Branding <IMicrosoftGraphOrganizationalBranding>]: organizationalBranding

[(Any) <Object>]: This indicates any property can be added to this object.

[BackgroundColor <String>]: Color that will appear in place of the background image in low-bandwidth connections. We recommend that you use the primary

color of your banner logo or your organization color. Specify this in hexadecimal format, for example, white is #FFFFFF.

[BackgroundImage <Byte[]>]: Image that appears as the background of the sign-in page. The allowed types are PNG or JPEG not smaller than 300 KB and not

larger than 1920 A- 1080 pixels. A smaller image will reduce bandwidth requirements and make the page load faster.

[BackgroundImageRelativeUrl <String>]: A relative URL for the backgroundImage property that is combined with a CDN base URL from the cdnList to provide

the version served by a CDN. Read-only.

[BannerLogo <Byte[]>]: A banner version of your company logo that appears on the sign-in page. The allowed types are PNG or JPEG no larger than 36 A- 245

pixels. We recommend using a transparent image with no padding around the logo.

[BannerLogoRelativeUrl <String>]: A relative url for the bannerLogo property that is combined with a CDN base URL from the cdnList to provide the

read-only version served by a CDN. Read-only.

[CdnList <String[]>]: A list of base URLs for all available CDN providers that are serving the assets of the current

resource. Several CDN providers are

used at the same time for high availability of read requests. Read-only.

[SignInPageText <String>]: Text that appears at the bottom of the sign-in box. You can use this to communicate additional information, such as the phone

number to your help desk or a legal statement. This text must be Unicode and not exceed 1024 characters.

[SquareLogo <Byte[]>]: A square version of your company logo that appears in Windows 10 out-of-box experiences (OOBE) and when Windows Autopilot is

enabled for deployment. Allowed types are PNG or JPEG no larger than 240 x 240 pixels and no more than 10 KB in size. We recommend using a transparent image with

no padding around the logo.

[SquareLogoRelativeUrl <String>]: A relative url for the squareLogo property that is combined with a CDN base URL from the cdnList to provide the version

served by a CDN. Read-only.

[UsernameHintText <String>]: String that shows as the hint in the username textbox on the sign-in screen. This text must be a Unicode, without links or

code, and can't exceed 64 characters.

[Id <String>]: The unique idenfier for an entity. Read-only.

[Localization <IMicrosoftGraphOrganizationalBrandingLocalization[]>]: Add different branding based on a locale.

[BackgroundColor <String>]: Color that will appear in place of the background image in low-bandwidth connections. We recommend that you use the primary

color of your banner logo or your organization color. Specify this in hexadecimal format, for example, white is #FFFFFF.

[BackgroundImage <Byte[]>]: Image that appears as the background of the sign-in page. The allowed types are PNG or JPEG not smaller than 300 KB and not

larger than 1920 A- 1080 pixels. A smaller image will reduce bandwidth requirements and make the page load faster.

[BackgroundImageRelativeUrl <String>]: A relative URL for the backgroundImage property that is combined with a CDN base URL from the cdnList to provide

the version served by a CDN. Read-only.

[BannerLogo <Byte[]>]: A banner version of your company logo that appears on the sign-in page. The allowed types are PNG or JPEG no larger than 36 A-

245 pixels. We recommend using a transparent image with no padding around the logo.

[BannerLogoRelativeUrl <String>]: A relative url for the bannerLogo property that is combined with a CDN base URL from the cdnList to provide the

read-only version served by a CDN. Read-only.

[CdnList <String[]>]: A list of base URLs for all available CDN providers that are serving the assets of the current resource. Several CDN providers are

used at the same time for high availability of read requests. Read-only.

[SignInPageText <String>]: Text that appears at the bottom of the sign-in box. You can use this to communicate additional information, such as the phone

number to your help desk or a legal statement. This text must be Unicode and not exceed 1024 characters.

[SquareLogo <Byte[]>]: A square version of your company logo that appears in Windows 10 out-of-box experiences (OOBE) and when Windows Autopilot is

enabled for deployment. Allowed types are PNG or JPEG no larger than 240 x 240 pixels and no more than 10 KB in size. We recommend using a transparent image with

no padding around the logo.

[SquareLogoRelativeUrl <String>]: A relative url for the squareLogo property that is combined with a CDN base URL from the cdnList to provide the

version served by a CDN. Read-only.

[UsernameHintText <String>]: String that shows as the hint in the username textbox on the sign-in screen. This text must be a Unicode, without links or

code, and can't exceed 64 characters.

[Id <String>]: The unique idenfier for an entity. Read-only.

[BusinessPhone <String[]>]: Telephone number for the organization. Although this is a string collection, only one number can be set for this property.

[CertificateBasedAuthConfiguration <IMicrosoftGraphCertificateBasedAuthConfiguration[]>]: Navigation property to manage certificate-based authentication

configuration. Only a single instance of certificateBasedAuthConfiguration can be created in the collection.

[Id <String>]: The unique idenfier for an entity. Read-only.

[CertificateAuthority <IMicrosoftGraphCertificateAuthority[]>]: Collection of certificate authorities which creates a trusted certificate chain.

[Certificate <Byte[]>]: Required. The base64 encoded string representing the public certificate.

[CertificateRevocationListUrl <String>]: The URL of the certificate revocation list.

[DeltaCertificateRevocationListUrl <String>]: The URL contains the list of all revoked certificates since the last time a full certificate revocaton

list was created.

[IsRootAuthority <Boolean?>]: Required. true if the trusted certificate is a root authority, false if the trusted

certificate is an intermediate

authority.

[Issuer <String>]: The issuer of the certificate, calculated from the certificate value. Read-only.

[IssuerSki <String>]: The subject key identifier of the certificate, calculated from the certificate value. Read-only.

[City <String>]: City name of the address for the organization.

[Country <String>]: Country/region name of the address for the organization.

[CountryLetterCode <String>]: Country or region abbreviation for the organization in ISO 3166-2 format.

[CreatedDateTime <DateTime?>]: Timestamp of when the organization was created. The value cannot be modified and is automatically populated when the

organization is created. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan

1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[Extension <IMicrosoftGraphExtension[]>]: The collection of open extensions defined for the organization. Read-only. Nullable.

[Id <String>]: The unique idenfier for an entity. Read-only.

[MarketingNotificationEmail <String[]>]: Not nullable.

[MobileDeviceManagementAuthority <MdmAuthority?>]: Mobile device management authority.

[OnPremisesLastSyncDateTime <DateTime?>]: The time and date at which the tenant was last synced with the on-premises directory. The Timestamp type

represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Read-only.

[OnPremisesSyncEnabled <Boolean?>]: true if this object is synced from an on-premises directory; false if this object was originally synced from an

on-premises directory but is no longer synced. Nullable. null if this object has never been synced from an on-premises directory (default).

[PostalCode <String>]: Postal code of the address for the organization.

[PreferredLanguage <String>]: The preferred language for the organization. Should follow ISO 639-1 Code; for example, en.

[PrivacyProfile <IMicrosoftGraphPrivacyProfile>]: privacyProfile

[(Any) <Object>]: This indicates any property can be added to this object.

[ContactEmail <String>]: A valid smtp email address for the privacy statement contact. Not required.

[StatementUrl <String>]: A valid URL format that begins with http:// or https://. Maximum length is 255 characters. The URL that directs to the company's

privacy statement. Not required.

[ProvisionedPlan <IMicrosoftGraphProvisionedPlan[]>]: Not nullable.

[CapabilityStatus <String>]: For example, 'Enabled'.

[ProvisioningStatus <String>]: For example, 'Success'.

[Service <String>]: The name of the service; for example, 'AccessControlS2S'

[SecurityComplianceNotificationMail <String[]>]:

[SecurityComplianceNotificationPhone <String[]>]:

[State <String>]: State name of the address for the organization.

[Street <String>]: Street name of the address for organization.

[TechnicalNotificationMail <String[]>]: Not nullable.

[TenantType <String>]:

[VerifiedDomain <IMicrosoftGraphVerifiedDomain[]>]: The collection of domains associated with this tenant. Not nullable.

[Capability <String>]: For example, Email, OfficeCommunicationsOnline.

[IsDefault <Boolean?>]: true if this is the default domain associated with the tenant; otherwise, false.

[IsInitial <Boolean?>]: true if this is the initial domain associated with the tenant; otherwise, false.

[Name <String>]: The domain name; for example, contoso.onmicrosoft.com.

[Type <String>]: For example, Managed.

[AddIn <IMicrosoftGraphAddIn[]>]: Defines custom behavior that a consuming service can use to call an app in specific contexts. For example, applications

that can render file streams may set the addIns property for its 'FileHandler' functionality. This will let services like Office 365 call the application in the

context of a document the user is working on.

[Api <IMicrosoftGraphApiApplication>]: apiApplication

[AppRole <IMicrosoftGraphAppRole[]>]: The collection of roles assigned to the application. With app role assignments, these roles can be assigned to users,

groups, or service principals associated with other applications. Not nullable.

[ApplicationTemplateId <String>]: Unique identifier of the applicationTemplate.

[CreatedOnBehalfOfDeletedDateTime <DateTime?>]:

[CreatedOnBehalfOfDisplayName <String>]: The name displayed in directory

[Description <String>]: An optional description of the application. Returned by default. Supports $filter (eq, ne, NOT, ge, le, startsWith) and $search.

[DisabledByMicrosoftStatus <String>]: Specifies whether Microsoft has disabled the registered application. Possible

values are: null (default value),

NotDisabled, and DisabledDueToViolationOfServicesAgreement (reasons may include suspicious, abusive, or malicious activity, or a violation of the Microsoft

Services Agreement). Supports $filter (eq, ne, NOT).

[FederatedIdentityCredentials <IMicrosoftGraphFederatedIdentityCredential[]>]: Federated identities for applications. Supports $expand and $filter (eq when

counting empty collections).

[GroupMembershipClaim <String>]: Configures the groups claim issued in a user or OAuth 2.0 access token that the application expects. To set this attribute,

use one of the following string values: None, SecurityGroup (for security groups and Azure AD roles), All (this gets all security groups, distribution groups, and

Azure AD directory roles that the signed-in user is a member of).

[HomeRealmDiscoveryPolicy <IMicrosoftGraphHomeRealmDiscoveryPolicy[]>]:

[IdentifierUri <String[]>]: The URIs that identify the application within its Azure AD tenant, or within a verified custom domain if the application is

multi-tenant. For more information, see Application Objects and Service Principal Objects. The any operator is required for filter expressions on multi-valued

properties. Not nullable. Supports $filter (eq, ne, ge, le, startsWith).

[Info <IMicrosoftGraphInformationalUrl>]: informationalUrl

[(Any) <Object>]: This indicates any property can be added to this object.

[MarketingUrl <String>]: Link to the application's marketing page. For example, https://www.contoso.com/app/marketing

[PrivacyStatementUrl <String>]: Link to the application's privacy statement. For example, https://www.contoso.com/app/privacy

[SupportUrl <String>]: Link to the application's support page. For example, https://www.contoso.com/app/support

[TermsOfServiceUrl <String>]: Link to the application's terms of service statement. For example, https://www.contoso.com/app/termsofservice

[IsDeviceOnlyAuthSupported <Boolean?>]: Specifies whether this application supports device authentication without a user. The default is false.

[IsFallbackPublicClient <Boolean?>]: Specifies the fallback application type as public client, such as an installed application running on a mobile device.

The default value is false which means the fallback application type is confidential client such as a web app. There are certain scenarios where Azure AD cannot

determine the client application type. For example, the ROPC flow where the application is configured without specifying a redirect URI. In those cases Azure AD

interprets the application type based on the value of this property.

[KeyCredentials <IMicrosoftGraphKeyCredential[]>]: The collection of key credentials associated with the application. Not nullable. Supports $filter (eq,

NOT, ge, le).

[CustomKeyIdentifier <Byte[]>]: Custom key identifier

[DisplayName <String>]: Friendly name for the key. Optional.

[EndDateTime <DateTime?>]: The date and time at which the credential expires.The Timestamp type represents date and time information using ISO 8601 format

and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z

[Key <Byte[]>]: Value for the key credential. Should be a base 64 encoded value.

[KeyId <String>]: The unique identifier (GUID) for the key.

[StartDateTime <DateTime?>]: The date and time at which the credential becomes valid.The Timestamp type represents date and time information using ISO

8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z

[Type <String>]: The type of key credential; for example, 'Symmetric'.

[Usage <String>]: A string that describes the purpose for which the key can be used; for example, 'Verify'.

[Logo <Byte[]>]: The main logo for the application. Not nullable.

[Note <String>]: Notes relevant for the management of the application.

[Oauth2RequirePostResponse <Boolean?>]:

[OptionalClaim <IMicrosoftGraphOptionalClaims>]: optionalClaims

[(Any) <Object>]: This indicates any property can be added to this object.

[AccessToken <IMicrosoftGraphOptionalClaim[]>]: The optional claims returned in the JWT access token.

[AdditionalProperty <String[]>]: Additional properties of the claim. If a property exists in this collection, it modifies the behavior of the optional

claim specified in the name property.

[Essential <Boolean?>]: If the value is true, the claim specified by the client is necessary to ensure a smooth authorization experience for the

specific task requested by the end user. The default value is false.

[Name <String>]: The name of the optional claim.

[Source <String>]: The source (directory object) of the claim. There are predefined claims and user-defined claims from extension properties. If the

source value is null, the claim is a predefined optional claim. If the source value is user, the value in the name property is the extension property from the

user object.

[IdToken <IMicrosoftGraphOptionalClaim[]>]: The optional claims returned in the JWT ID token.

[Saml2Token <IMicrosoftGraphOptionalClaim[]>]: The optional claims returned in the SAML token.

[ParentalControlSetting <IMicrosoftGraphParentalControlSettings>]: parentalControlSettings

[(Any) <Object>]: This indicates any property can be added to this object.

[CountriesBlockedForMinor <String[]>]: Specifies the two-letter ISO country codes. Access to the application will be blocked for minors from the countries

specified in this list.

[LegalAgeGroupRule <String>]: Specifies the legal age group rule that applies to users of the app. Can be set to one of the following values:

ValueDescriptionAllowDefault. Enforces the legal minimum. This means parental consent is required for minors in the European Union and

Korea.RequireConsentForPrivacyServicesEnforces the user to specify date of birth to comply with COPPA rules. RequireConsentForMinorsRequires parental consent for

ages below 18, regardless of country minor rules.RequireConsentForKidsRequires parental consent for ages below 14, regardless of country minor

rules.BlockMinorsBlocks minors from using the app.

[PasswordCredentials <IMicrosoftGraphPasswordCredential[]>]: The collection of password credentials associated with the application. Not nullable.

[CustomKeyIdentifier <Byte[]>]: Do not use.

[DisplayName <String>]: Friendly name for the password. Optional.

[EndDateTime <DateTime?>]: The date and time at which the password expires represented using ISO 8601 format and is always in UTC time. For example,

midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Optional.

[KeyId <String>]: The unique identifier for the password.

[StartDateTime <DateTime?>]: The date and time at which the password becomes valid. The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Optional.

[PublicClient <IMicrosoftGraphPublicClientApplication>]: publicClientApplication

[(Any) <Object>]: This indicates any property can be added to this object.

[RedirectUri <String[]>]: Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where

OAuth 2.0 authorization codes and access
tokens are sent.

[RequiredResourceAccess <IMicrosoftGraphRequiredResourceAccess[]>]: Specifies the resources that the application needs to access. This property also
specifies the set of OAuth permission scopes and application roles that it needs for each of those resources. This configuration of access to the required
resources drives the consent experience. Not nullable. Supports $filter (eq, NOT, ge, le).

[ResourceAccess <IMicrosoftGraphResourceAccess[]>]: The list of OAuth2.0 permission scopes and app roles that the application requires from the specified
resource.

[Id <String>]: The unique identifier for one of the oauth2PermissionScopes or appRole instances that the resource application exposes.

[Type <String>]: Specifies whether the id property references an oauth2PermissionScopes or an appRole. Possible values are Scope or Role.

[ResourceAppId <String>]: The unique identifier for the resource that the application requires access to. This should be equal to the appId declared on
the target resource application.

[SignInAudience <String>]: Specifies the Microsoft accounts that are supported for the current application. Supported values are: AzureADMyOrg,
AzureADMultipleOrgs, AzureADandPersonalMicrosoftAccount, PersonalMicrosoftAccount. See more in the table below. Supports $filter (eq, ne, NOT).

[Spa <IMicrosoftGraphSpaApplication>]: spaApplication

[(Any) <Object>]: This indicates any property can be added to this object.

[RedirectUri <String[]>]: Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where OAuth 2.0 authorization codes and access
tokens are sent.

[Tag <String[]>]: Custom strings that can be used to categorize and identify the application. Not nullable.Supports $filter (eq, NOT, ge, le, startsWith).

[TokenEncryptionKeyId <String>]: Specifies the keyId of a public key from the keyCredentials collection. When configured, Azure AD encrypts all the tokens
it emits by using the key this property points to. The application code that receives the encrypted token must use the matching private key to decrypt the token
before it can be used for the signed-in user.

[TokenIssuancePolicy <IMicrosoftGraphTokenIssuancePolicy[]>]:

[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:

[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy. The syntax for the definition

differs for each derived policy type. Required.

[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be

activated as the organization default. Optional, default value is false.

[Description <String>]: Description for this policy.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[TokenLifetimePolicy <IMicrosoftGraphTokenLifetimePolicy[]>]: The tokenLifetimePolicies assigned to this application. Supports $expand.

[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:

[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy. The syntax for the definition

differs for each derived policy type. Required.

[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be

activated as the organization default. Optional, default value is false.

[Description <String>]: Description for this policy.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[Web <IMicrosoftGraphWebApplication>]: webApplication

[(Any) <Object>]: This indicates any property can be added to this object.

[HomePageUrl <String>]: Home page or landing page of the application.

[ImplicitGrantSetting <IMicrosoftGraphImplicitGrantSettings>]: implicitGrantSettings

[(Any) <Object>]: This indicates any property can be added to this object.

[EnableAccessTokenIssuance <Boolean?>]: Specifies whether this web application can request an access token using the OAuth 2.0 implicit flow.

[EnableIdTokenIssuance <Boolean?>]: Specifies whether this web application can request an ID token using the OAuth 2.0 implicit flow.

[LogoutUrl <String>]: Specifies the URL that will be used by Microsoft's authorization service to logout an user

using front-channel, back-channel or SAML

logout protocols.

[RedirectUri <String[]>]: Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where OAuth 2.0 authorization codes and access

tokens are sent.

[DataType <String>]: Specifies the data type of the value the extension property can hold. Following values are supported. Not nullable. Binary - 256 bytes

maximumBooleanDateTime - Must be specified in ISO 8601 format. Will be stored in UTC.Integer - 32-bit value.LargeInteger - 64-bit value.String - 256 characters

maximum

[Name <String>]: Name of the extension property. Not nullable.

[TargetObject <String[]>]: Following values are supported. Not nullable. UserGroupOrganizationDeviceApplication

[Description <String>]: Description for this policy.

[AppliesTo <IMicrosoftGraphDirectoryObject[]>]:

[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy. The syntax for the definition

differs for each derived policy type. Required.

[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be

activated as the organization default. Optional, default value is false.

[Definition <String[]>]: A string collection containing a JSON string that defines the rules and settings for a policy. The syntax for the definition differs

for each derived policy type. Required.

[IsOrganizationDefault <Boolean?>]: If set to true, activates this policy. There can be many policies for the same policy type, but only one can be activated

as the organization default. Optional, default value is false.

[Description <String>]: Description for this policy.

[DeletedDateTime <DateTime?>]:

[DisplayName <String>]: The name displayed in directory

[IdentifierUri <String[]>]: The URIs that identify the application within its Azure AD tenant, or within a verified custom domain if the application is

multi-tenant. For more information, see Application Objects and Service Principal Objects. The any operator is required for filter expressions on multi-valued

properties. Not nullable. Supports $filter (eq, ne, ge, le, startsWith).

[Info <IMicrosoftGraphInformationalUrl>]: informationalUrl

[IsDeviceOnlyAuthSupported <Boolean?>]: Specifies whether this application supports device authentication without a user. The default is false.

[IsFallbackPublicClient <Boolean?>]: Specifies the fallback application type as public client, such as an installed application running on a mobile device. The

default value is false which means the fallback application type is confidential client such as a web app. There are certain scenarios where Azure AD cannot

determine the client application type. For example, the ROPC flow where the application is configured without specifying a redirect URI. In those cases Azure AD

interprets the application type based on the value of this property.

[KeyCredentials <IMicrosoftGraphKeyCredential[]>]: The collection of key credentials associated with the application. Not nullable. Supports $filter (eq, NOT,

ge, le).

[Logo <Byte[]>]: The main logo for the application. Not nullable.

[Note <String>]: Notes relevant for the management of the application.

[Oauth2RequirePostResponse <Boolean?>]:

[OptionalClaim <IMicrosoftGraphOptionalClaims>]: optionalClaims

[ParentalControlSetting <IMicrosoftGraphParentalControlSettings>]: parentalControlSettings

[PasswordCredentials <IMicrosoftGraphPasswordCredential[]>]: The collection of password credentials associated with the application. Not nullable.

[PublicClient <IMicrosoftGraphPublicClientApplication>]: publicClientApplication

[RequiredResourceAccess <IMicrosoftGraphRequiredResourceAccess[]>]: Specifies the resources that the application needs to access. This property also specifies

the set of OAuth permission scopes and application roles that it needs for each of those resources. This configuration of access to the required resources drives

the consent experience. Not nullable. Supports $filter (eq, NOT, ge, le).

[SignInAudience <String>]: Specifies the Microsoft accounts that are supported for the current application. Supported values are: AzureADMyOrg,

AzureADMultipleOrgs, AzureADandPersonalMicrosoftAccount, PersonalMicrosoftAccount. See more in the table below. Supports $filter (eq, ne, NOT).

[Spa <IMicrosoftGraphSpaApplication>]: spaApplication

[Tag <String[]>]: Custom strings that can be used to categorize and identify the application. Not nullable. Supports

$filter (eq, NOT, ge, le, startsWith).

[TokenEncryptionKeyId <String>]: Specifies the keyId of a public key from the keyCredentials collection. When configured, Azure AD encrypts all the tokens it

emits by using the key this property points to. The application code that receives the encrypted token must use the matching private key to decrypt the token

before it can be used for the signed-in user.

[TokenIssuancePolicy <IMicrosoftGraphTokenIssuancePolicy[]>]:

[TokenLifetimePolicy <IMicrosoftGraphTokenLifetimePolicy[]>]: The tokenLifetimePolicies assigned to this application. Supports $expand.

[Web <IMicrosoftGraphWebApplication>]: webApplication

KEYCREDENTIALS <MicrosoftGraphKeyCredential[]>: key credentials associated with the application.

[CustomKeyIdentifier <Byte[]>]: Custom key identifier

[DisplayName <String>]: Friendly name for the key. Optional.

[EndDateTime <DateTime?>]: The date and time at which the credential expires.The Timestamp type represents date and time information using ISO 8601 format and

is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z

[Key <Byte[]>]: Value for the key credential. Should be a base 64 encoded value.

[KeyId <String>]: The unique identifier (GUID) for the key.

[StartDateTime <DateTime?>]: The date and time at which the credential becomes valid.The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z

[Type <String>]: The type of key credential; for example, 'Symmetric'.

[Usage <String>]: A string that describes the purpose for which the key can be used; for example, 'Verify'.

PASSWORDCREDENTIALS <MicrosoftGraphPasswordCredential[]>: Password credentials associated with the application.

[CustomKeyIdentifier <Byte[]>]: Do not use.

[DisplayName <String>]: Friendly name for the password. Optional.

[EndDateTime <DateTime?>]: The date and time at which the password expires represented using ISO 8601 format and is always in UTC time. For example, midnight

UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Optional.

[KeyId <String>]: The unique identifier for the password.

[StartDateTime <DateTime?>]: The date and time at which the password becomes valid. The Timestamp type represents date and time information using ISO 8601

format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Optional.

---------- EXAMPLE 1 ----------

PS C:\># ObjectId is the string representation of a GUID for directory object, application, in Azure AD.

$Id = "00000000-0000-0000-0000-000000000000"

$cert is Base64 encoded content of certificate

$credential = New-Object -TypeName "Microsoft.Azure.PowerShell.Cmdlets.Resources.MSGraph.Models.ApiV10.MicrosoftGraphKeyCredential" `

-Property @{'Key' = $cert;

'Usage' = 'Verify';

'Type' = 'AsymmetricX509Cert'

}

New-AzADAppCredential -ObjectId $Id -KeyCredentials $credential

---------- EXAMPLE 2 ----------

PS C:\># ApplicationId is AppId of Application object which is different from directory id in Azure AD.

Get-AzADApplication -ApplicationId $appId | New-AzADAppCredential -StartDate $startDate -EndDate $endDate

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.resources/new-azadappcredential